Revisiting Past Cyber Security Recommendations: Lessons we Have Failed to Learn

Matthias Schulze and Jantje Silomon
Institute for Peace Research and Security Policy (IFSH), Hamburg, Germany

schulze@ifsh.de
silomon@ifsh.de

Abstract: Cyber-security is constantly evolving as new technologies introduce new vulnerabilities and threat actors constantly develop new techniques to penetrate systems. Much focus in scholarship is on the cyber-offense, while few analyse changes in the cyber-defence posture. Since its inception, defensive information security has evolved and introduced a plethora of new security controls to either prevent, detect, mitigate, or respond to new cyber-attacks. When studying cyber-incidents, a paradox becomes apparent: often, low-end security fails are responsible for most breaches, such as default system configurations and credentials or violations of the principle of least privileges. Even security sensitive organisations such as the US DoD or IT companies suffer from this paradox, as a recent NSA/CISA report indicates: large sums are spent on high-end security programs only to be compromised by low-end attacks. This paradox becomes even more pronounced when introducing a longitudinal historical perspective: many of these issues have been known for decades, as reports from the 1970s show. These include inadequate hardware and software not designed with security in mind, the issue of managing resource access controls in a multi-user environment that includes remote terminals (aka a cloud infrastructure), malicious insider threats that bypass security controls, as well as the issue of applying timely software patches. In sum: while the IT security industry is rushing to introduce new high-level security controls and technologies, the main issues seem to be age-old problems and the failure to learn lessons from the past, warranting a historical approach. In this paper, the origin of security controls is examined, shedding light on relevant best practices, recommendations and why they emerged. Starting in the 1960s, we analyse the emerging technologies of each subsequent decade, explore what changes in IT-security controls these new technologies necessitated, and how IT and later cyber-security changed over the years. Furthermore, reference is made to the aftermath of selected cyber-attacks to further highlight is analysed to explore potential shifts in security paradigms beyond those introduced by technology itself.

Keywords: History of IT Security, Security Controls, Lessons Learned

1. Introduction

The rapid development of technology invariably introduces new vulnerabilities and risks, forcing IT-security to constantly readjust. Attackers strive to discover new attack techniques to exploit systems, while defenders must adapt and introduce new security controls to manage emerging risks. When studying the history of IT-security, a paradox emerges. Often, it is not the novel, cutting-edge exploits that lead to compromise, but the failure to implement baseline security controls – those that have been known for decades. Despite technology advancing and its accompanying attack surface growing, certain security controls appear almost unchanged since their inception. Not only are they relevant but vital and include concepts such as password policies, authentication, access control, separation of users and programs, as well as adequate backup strategies.

More specifically, security controls are defined as "safeguards or countermeasures prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements" (NIST 2020, p.63). Generally, security controls are distinguished either by *type* (physical, technical, or administrative), *function* (preventative, detective, corrective, deterrent, or compensating) or *level* upon which they are decided and implemented (management, operational, or technical) (Viegas, Kuyucu, 2022).

Another way to categorise controls is by their intricacy. *Low-end security controls* (sometimes called *baseline* or *essential* controls) typically cost little in terms of computational, financial, as well as human resources to implement. The US National Institute of Standards and Technology (NIST) defines an IT security control baseline as the "set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system" (NIST, 2020 p.63). They are Pareto-optimised, achieving "80% of the benefit from 20% of the effort", meaning they protect against most cyber threats (CCCS, 2020). In adopting controls, the best practice has been to follow established security frameworks that select and implement several different controls, all dependent on the envisaged security objectives, risk appetite, and compliance requirements.

Yet, many organisations still fail to implement these basic, age-old security controls, as a 2023 study by the US National Security Agency highlights: the majority of the top 10 security misconfigurations discovered among government networks in the US include the failure to implement baseline security controls such as having

insecure default configurations and improper separation of user and administrator privilege (CISA, 2023). Even cyber-security sensitive organisations are prone to such failures.

In this paper, we process-trace the history of IT-security controls and analyse why they were introduced, and how they have changed over time. We focus on defensive security practices and technical controls, from which we then derive core IT-security lessons that many have still not learned. The next section explores the concept of security controls, followed by a chapter on the history of IT-security across the past five decades, including relevant security best practices and recommendations, as well as selective cyber-incidents. The outcomes are then summarised and discussed.

2. Security Controls Through the Decades

While the conceptual delineation of security controls is widely known because of standards such as ISO, less is known about the origin of these controls. The section explores how emerging technologies of past decades (1960-2010s) introduced the need for new security measures, focussing on physical, technical, and administrative controls. We take a chronological approach ending with the year 2020, as the current decade and its technological developments, such as the rise of generative AI, is still unfolding.

2.1 1960s: Minicomputers and Multi-User Time Sharing

The first computers were developed during the 1940s in the context of World War II. They were predominately built in a governmental, national security context. Security paradigms of the time focused on isolating these room-sized calculating machines, preventing theft, sabotage, and vandalism, while security controls centred on preventing physical access through guards, fences, and checkpoint stations (Yost, 2007). Integrated circuits in the 1960s were a game changer, improving and shrinking “mini computers” such as the PDP-1. Improved magnetic storage, new programming languages and new input methods via terminals lead to a wider adoption at universities and private companies.

The invention of *multi-user time-sharing* at MIT in 1961 was arguably the most IT-security relevant invention of this decade (Freiberger and Swaine, no date). Time-sharing allowed for multitasking and the simultaneous running of programs by different users at the same time (Meijer et al., 2007). However, this also led to the “core” security problem that still plagues society today: “with multiprogramming the confidentiality, integrity and availability of one program could be under attack by an arbitrary concurrently running program” (Meijer et al., 2007). In essence, an uncleared user or a single program could potentially read or alter the content of other programs residing in the same memory, a particular concern within national security contexts and demonstrated by the DARWIN computer game in 1961 (Vyssotsky, 1961). One of the first technical controls to remedy this was the introduction of the user password in 1961 to separate time-sharing accounts on the same machine (Beyond Identity, 2021).

A now famous study on security controls was conducted by Willis H. Ware in the late 1960s, which was later declassified. He described the security threats emanating from the lack of technical isolation between programs in shared memory, from accidental data disclosure and covert infiltration to the possibility of hijacked remote-terminals and brute-forcing of weak access codes, among numerous others. The “Ware Report” (Ware, 1970) introduced a plethora of security controls to tackle these problems, many of which are still familiar today, including:

- separation of users and processes with different access permissions
- technical implementation of read/write permissions based on user privilege levels
- user authentication
- event logging and audit trails of all transactions
- automatic self-testing system processing
- secure data deletion
- constant system certification

The report called for a security by design principle, arguing that the operating system must support user and program separation, controlled by a supervisor program that runs with elevated privileges and manages user, file and program access control (ibid). Some of the proposed controls were only theoretical at the time, for example file and storage encryption, which did not become technically feasible until later (Brenner, 2007). While the report remained classified until 1975, many developers discovered the issues independently and began work to mitigate them, such as ideas on file access control and data labelling (MIT, no date).

2.2 1970s: Networks, Reference Monitors, and Encryption

Two major trends dominated this decade: the commercialisation of small, personal computers such as the Xerox Alto (1974), the Altair 8800 (1975), or Apple 1 (1976) and the rise of networking. The latter included the expansion of the ARPANET and the development of the Ethernet in 1973, as well as many other proprietary networking standards. The creation of the TCP/IP protocol provided the foundation for the networking of networks (1974). Internetworking created demand for new applications such as email (1971), remote login via TELNET (1973), and early online newsgroups such as Usenet in 1978.

Wider societal adoption of smaller, now networked computers, led to a dramatic increase in the user base and expanded the attack surface. In addition to lacking security controls and the still unresolved core computer security problem of the 1960s, networking in particularly added a new layer of problems: most early protocols prioritised reliability, redundant channels, availability, and performance over security, as they did not feature authentication, integrity, or confidentiality protections (DeNardis, 2007). Early “hacks” or student pranks gone wrong highlighted the security issues introduced by networking, such as when the CREEPER worm spread through the ARPANET before being stopped by the REAPER worm in 1971, arguably the first anti malware tool (Bales, 2023).

In 1972, the Anderson report (Anderson, 1972), raised some fundamental security issues still prevalent today. Anderson diagnosed that many systems designers did not account for a hostile operating environment or malicious insiders during the design process, and that many commercial systems had exploitable implementation flaws if programming access could be gained. Retrofitting security, including ad hoc patches fixing vulnerabilities, were not considered sufficient. Instead, Anderson aimed for a structured approach, by first developing a standard model to measure the security of a system, and further argued for a central reference monitor that would manage access relationships between users and objects. He also called for certification, as well as a risk management approach to security.

During the 1970s, the various challenges in computer security prompted researchers to seek solutions through technological advancements. These efforts gave rise to the development of the principle of the least privilege (Linden, 1976) and the pursuit of mathematically provable security in operating systems and kernels (Neumann et al., 1975). Concurrently, Bell and Lapadula proposed a computer security model (Yost, 2007). The growing use of computers in business raised apprehensions about the security and privacy of commercial data, leading IBM to introduce the Systems Network Architecture in 1974, which integrated telecommunication and database management while incorporating access control to network resources (Computer History Museum, no date). Additionally, concerns emerged regarding wiretapping and on-path data alterations with the networking of database access. Furthermore, data availability issues spurred the initial implementation of backup and restoration strategies. Insecure networking channels and the threat of espionage contributed to many advances in cryptography: the Data Encryption Standard (DES), Whitfield Diffie and Martin Hellman’s work on asymmetric encryption (1976), and Rivest, Shamir and Adleman’s RSA algorithm in 1977 (Yost, 2007).

Lastly, the wider adoption of cheaper computers introduced hacker culture into mainstream society (Brenner, 2007), with the first Bulletin Board Systems (1978) facilitating the exchange of early malware and tools, techniques, and procedures to exploit internetworked systems.

2.3 1980s: Routing, Logging, and IDS

The technological changes of the 1980s represent mostly an evolution and consolidation of earlier trends: various personal computing companies such as Apple and IBM competed until the latter’s domination with the help of Microsoft DOS. Similarly, various networking standards such as Token Ring, TCP/IP, OSI and IBM’s SNA competed, until TCP/IP and Ethernet took the lead (Piscitello and Chapin, 1993).

Networking personal computers increased the attack surface, with over 100,000 ARPANET hosts being connected without fundamental security controls by the end of the decade (Computer History Museum, no date). The first security incidents such as the Morris worm in 1988 made headlines, but also led to the introduction of a core operational security control: the creation of Computer Emergency Response Teams and the creation of incident response strategies (DeNardis, 2007). First academic work (Cohen, 1987), and industry products dealt with computer viruses, such as Anti4us and Flushot (1987). Meanwhile, the US DoD founded their first Computer Security Center in 1981 and funded related projects such as the “Rainbow Series” of IT-security books, as well as the development of secure networking protocols.

In the 1980s, the management and protection of the increasing number of computer networks and hosts against external threats became a primary focus for new security controls. The release of Syslog for UNIX in 1980 established a standard for message logging across various networking devices, while network gateways and routers were deployed to manage external access to internal networks. The first Cisco router with access control capabilities, enabling the blocking of specific network addresses, was introduced in 1985 (Lewis, 2024). Additionally, the adoption of network segregation based on target audience and use cases gained momentum, exemplified by the US Department of Defence's separation of its military network Milnet from the public ARPANET in 1988 (Perry, Blumenthal, and Hinden, 1988). Furthermore, the concept of Virtual Local Area Networks (VLANs) proposed by David Sincoskie in 1984 for network performance management evolved into a fundamental technical security control for isolating network segments (Vance, 2022).

Another network security concern was the lack of visibility or a log trail of malicious actors entering a network. This led to research on determining the origin of IP data packets and network intrusion detection (NIDS) systems (Bace, 2012). Around the same time, the first commercial traffic scanning technology called Netranger began to use signatures for detecting malicious network traffic.

2.4 1990s: World Wide Web

The 1990s saw the emergence of the World Wide Web and the global expansion of the TCP/IP-based Internet, which influenced a wide range of new technologies, including business-to-business networks, the client-server architecture, and home computing (Biene-Hershey, 2007). Industry-specific software, such as Windows NT, introduced numerous security controls, such as client-side event logs, per-object access control lists, and the NTFS file system supporting data encryption and permission-based access control (Awati, 2023). However, personal computer security was not a primary concern, leading to the prevalence of viruses throughout the decade (Brenner, 2007). The lack of security in transmission protocols and the widespread use of email attachments, exemplified by the Melissa Virus, contributed to this trend. Additionally, the internet introduced a new threat category: web-based attacks. The latter half of the decade witnessed an increase in rogue proxy servers, malicious websites, and drive-by infections of web clients, while emerging e-commerce faced its first Denial of Service (DoS) attacks and various fraud schemes (ibid).

Meanwhile, (inter-)network security also advanced, with early IP encryption research later evolving into IPsec, SSL was introduced for web traffic encryption by Netscape in 1994, and SSH became a secure alternative to Telnet a year later. Microsoft's Point-to-Point protocol to secure a connection between a client and a server laid the foundation for secure tunnels, which would later become known as Virtual Private Networks (Mujović, 2018). In 1995, Verisign was founded as a Digital Certificate Authority, allowing for a web server to demonstrate authenticity to a client, opening the door for an entire industry. Lastly, the now obsolete Wired Equivalent Privacy (WEP) was introduced to encrypt wireless network traffic in 1997, as freely available packet capture and traffic analysis software, such as Wireshark or Snort, introduced the need to secure wireless traffic.

Corporate networks were faced with authentication questions regarding network external clients and managing privacy and integrity of corporate data (Brenner, 2007), problems which were summarised in the "Computers at Risk" study by the US National Research Council (National Science Foundation, 1991). While solutions included commercial first generation stateful Firewall systems (Bellovin et al., 1994), they popularised the simplified security assumption: that the internal network is trustworthy, while the outside is not (Biene-Hershey, 2007). Screened subnets (Demilitarized Zones) to segregate web-facing servers from private networks with firewalls on the edges were another essential security control that became a mainstay.

The 1990s also marked the first standardisation attempts of many of the previously discussed security controls: the British "Code of Practice for Information Security Management" developed by industry actors and published in 1993. It asked for the development of a security policy, the creation of a security organisation within a company, asset classification, personnel security, physical security, network management, system access control, secure system development, business continuity planning and compliance. The code of practice later expanded and developed into the BS 7799/ISO standard (von Solms, 1998).

Lastly, IT-security emerged as a business model and cyber-security emerged as a distinct topic towards the end of the decade. As networked computers began to control more and more critical infrastructure, some think tanks began to write about the possibility of "cyber warfare" in the context of interstate rivalry (Arquilla and Ronfeldt, 1993). The Y2k bug and the first congressional hearings in the US increased the public's awareness of IT-insecurity. Meanwhile, the first state-linked cyber-incidents came to light, such as the Rome Labs at Griffiss Air

Force Base (1994). In 1997, NSA's Eligible Receiver cyber-attack simulation highlighted the issue of IT-security as a matter of national security (Schulze, 2018).

2.5 2000s: Mobile Devices and Web 2.0

Mobile devices, such as smaller notebooks, early BlackBerries and Palm-handsets, the first iPhone in 2007, Android as an open-source OS in 2008, and mobile-networking (802.11 Wi-Fi and 3G) changed security. Securing a network perimeter with devices moving in and out suddenly became much harder. As a result, security controls such as port-based network access control (NAC or 802.1X), remote authentication of users via RADIUS or Kerberos became essential during the 2000s (IEEE Standards Association, 2023). While Windows 2000 introduced many of these technologies in the form of Active Directory for a wider enterprise audience, consumer-level security was still lacking. In 2001, Windows XP shipped without a firewall, and was only added later.

The internet became ubiquitous, filled with advertising and commerce. Web 2.0 and Social media emerged, with Facebook (2004), YouTube (2005), and Twitter (2006), introducing additional attack vectors, such as social engineering and scamming. User account management and password policies became essential security controls, particularly with new web-services, such as file hosting or digital payments. While two-factor authentication (2FA) was not new, it became more user-friendly due to mobile devices (de Fremery, 2021).

The rise in global internet users in the 2000s led to a surge in new malware, including notable cases such as ILOVEYOU, Slammer, and CodeRed (Brenner, 2007). This era also saw the emergence of botnets (Storm) and larger scale distributed Denial of Service (DDoS) attacks. In response, best practices against DDoS attacks included network ingress filtering and load-balancing (Ferguson and Senie, 2000). Early Firewalls, suddenly ineffective against web attacks, gained stateful inspection capabilities and application-layer awareness. Additionally, the first active Intrusion Prevention Systems, capable of modifying network transmissions, emerged alongside advancements in client-side Antivirus software, which shifted to include heuristics and behavioural analysis for improved detection of malware vectors (ibid).

Different security solutions introduced another security challenge: their greater number and complexity made it harder for organisations to design coherent security architectures. This created the need for the first Unified Thread Management systems that combined many of the technologies in one package. Additionally, security technology was not without its flaws, necessitating vulnerability management and scanning practices (Drake, 2020). To aid this process, the Common Vulnerability Scoring System was released in 2005. This was also mirrored by many best practice recommendations on information security controls, which were released in the 2000s, such as ISO/IEC 17799 (later ISO/IEC 27002), the NIST Risk Management Framework and additional cloud security controls (ISO/IEC 27017). These aimed to streamline security and help to manage the new complexities of IT-security.

By the end of the decade, some arrived at the conclusion that achieving security is infeasible, and the "assume breach" paradigm began to gain traction (Hayden, 2009). This was facilitated by the increasing professionalisation of cyber crime and state-sponsored threat actors, pushing cyber-warfare as a theme in national security strategies and contexts. Noteworthy in this regard are the 2007 Estonia DDoS attacks, which led to the creation of the NATO CCDCOE in Tallinn. In the same year, the Aurora Generator Test showed that malware can cause physical destruction of a generator, foreshadowing things to come (Schulze, 2018).

2.6 2010s: Cloud, IoT, Smartphone Ubiquity, and Advanced Persistent Threats

Moving on-perimeter services to cloud environments such as Amazon Web Services or Microsoft Azure in the 2010s gave rise to the "as-a-service" industry. At the same time, the Internet of Things (IoT) expanded exponentially, including anything from wearables to industrial machines.

This decade also saw an evolution of cyber-attacks. First, the decade witnessed an enormous proliferation of cybercrime, with significant increases in ransomware and business email compromise, the former seizing the monetisation opportunity provided by cryptocurrencies. Ransomware started out with a 'spray and pray' style of targeting, focusing on many small targets, but began to shift towards 'big-game hunting' of lucrative targets at the end of the decade. The cybercrime ecosystem also professionalised with "as a service" models for renting Botnets, malware (such as Gameover Zeus) and other command and control infrastructure. Second, we witnessed the rise of "destructive" cyber-attacks that caused enormous (financial) damage: in 2013 the Shamoon wiper permanently deleted data at Saudi Aramco, one of the largest oil companies in the world. In

2017, WannaCry caused havoc globally, particularly in the UK, temporarily crippling the NHS – to make matters worse, it propagated via the EternalBlue exploit, which had originally been developed by the NSA. In the same year, (Not)Petya targeted Ukraine but had far lager ramifications, such as hitting the Danish shipping company Maersk. Third, data breaches and state-sponsored cyber-espionage also became an established intelligence practice, exemplified by the 2013 Snowden leaks or the breach of the US Office of Personnel Management and Budget in 2015. Fourth, state-driven cyber-operations escalated by targeting industrial control systems of critical-infrastructure. Highly sophisticated attacks such as Stuxnet or Duqu (2010), which utilised previously unknown zero-day vulnerabilities, inspired more states to develop sophisticated offensive cyber-capabilities (Sanger 2018). Countries such as China, Russia, Iran, and North Korea emerged as formidable cyber powers. To describe this increasingly complex threat landscape and sophistication of attacker profile, the term Advanced Persistent Threat (APT) was coined, and by the end of the decade hundreds of such groups were tracked by security companies (Schneier 2018). Fifth, to address the demand of states for cyber-capabilities, private companies such as the NSO group began to sell commercial spy-ware at scale.

To make sense of this increasingly complex attacker landscape, MITRE and private security vendors launched several threat intelligence initiatives and platforms. This was based on the realisation that cooperating with others and sharing real-time knowledge could combat APTs. The MITRE ATT&CK framework standardised the analytical description of cyber-attack stages (2013). For defenders, ingesting, analysing, and sharing threat intelligence with SIEM platforms via the STIX standard (2013), and setting-up Security Operations Centres became essential security controls. At the same time, exploit acquisition platforms began to emerge, such as Zerodium or Crowdfense, offering premiums for zero-days before selling them to governments or other interested parties, counter to bug-bounty programmes and platforms, which also expanded rapidly. Additionally, vulnerability and patch management, as well as open-source intelligence, became necessary in dealing with advanced threats. Lastly, big IT security companies started publishing detailed reports on APT behaviour, targeting and tools, techniques, and procedures to aid defenders in detection and response.

The cloud challenged the perimeter-based security model, where everything “inside” was essentially considered safe. In 2010, John Kindervag presented his concept of “Zero Trust”, a model that mandates users and devices are verified and secured before gaining access to any resource (Kindervag, 2016). Three core tenets call for all resources to be verified and secured, access controls to be limited and strictly controlled, and lastly, all network traffic to be inspected and logged. While the notion of security by design was deliberated since the 1970s, the concept of DevOps put it into practice. This shift ensures that security concerns become integrated into every stage of code development, from design to deployment, thus allowing vulnerabilities to be identified and mitigated at an earlier stage (Zioni, 2022).

3. Conclusion

In this paper, we traversed over half a century of IT security controls: after WW2, the introduction of integrated circuits shifted the focus on security beyond simple physical security controls. The 1960s gave rise to the core security problem, and an awareness of lacking isolation between system processes, as well as the failure to design software with security in mind. In the next decade, researchers believed these all to be solvable engineering problems, with hopes of achieving provable security, for example in the form of a mathematically trusted system kernel. However, they did not account for technology to leap forward, with the 1980s seeing a rapid increase in networking coupled with a rise of commercial and private computers – all of which were fundamentally insecure machines.

Yet, this paled in comparison to the 1990s and the advent of the World Wide Web, its insecure networking protocols and vulnerable web servers creating an immense new attack surface. Hopes of isolating systems and securing the network perimeter against new threats proved to be a flawed assumption – the introduction of mobile devices alone made such an approach untenable.

In the early 2000s, a paradigm shift occurred, turning security considerations from being an afterthought to an integral part of IT design and use. Standards were publicised, but adoption was slow and the advent of the cloud, IoT, and an enormous professionalisation of attackers dampened hopes of overcoming security challenges by adding greater levels of complexity. The assumption, that it is indeed possible to fully secure a network, slowly shifted to the assume breach paradigm: dealing with an attacker that had already bypassed security controls. Following major supply chain attacks, this was reflected by the growing zero-trust paradigm push and its adoption: no entity within a network can be trusted.

While security controls had to adjust to technological changes, the underlying principles still hold true, from ideas of the least privilege to strong, (multi-)authenticated password. It is still striking that many of the IT-security problems we face today are essentially iterations of problems that have been described in the early 1970s by Ware and Anderson – yet we still fail at implementing them.

Adopting a historical approach allowed us to shed light on the underlying dynamic: each decade introduced a new set of core technologies all of which ushered in new security threats, while, at the same time, the vulnerabilities of the previous generation of technology have not been completely remedied. As a result, organisations must manage several generations of technology, often to the point of running numerous legacy systems that have long reached their end-of-life or end-of-service, not to mention having personnel qualified on such systems. The problem today is not a lack of knowledge of how to build secure systems or the lack of solutions, as it was in the 1970s. Instead, it is one of complexity, of user complacency, and the mixture of still insecure legacy and new technologies. This is particularly well illustrated by the 2010s, where the primary innovations of IT-security were tools to organise knowledge and to manage complexity, including SIEM, threat intelligence platforms, and vulnerability management processes. A primary goal for the next decade should thus be to make security simpler: not adding new technologies on top, but rather rebuilding systems as simple and secure as possible. Trends such as "security by design", SecDevOps, and "Zero Trust" are promising, but only if they lead to a complete redesign of systems, from the ground up. Interestingly, this is the same recommendation as that of the 1970s Anderson report.

Since we focused predominantly looked primarily on technical aspects of security, future research should analyse processes and the evolution of administrative and organisational security controls, not just the evolution of technical controls. It appears that one reason why organisations struggle with managing complexity is that they have bad processes and administrative controls in place. However, processes are much harder to change than just buying the latest technological quick fix. We encourage future research to trace the evolution of administrative controls in more detail to fill this gap.

References

Anderson, J. P. (1972) *Computer Security Technology Planning Study*, United Stated of America, Department of Defense.

Arquilla, J. and Ronfeldt, D. (1993) Cyberwar is Coming! *RAND Corporation*, Santa Monica, CA.

Awati, R. (2023) "Definition: Windows NT", [online], *TechTarget*, https://www.techtarget.com/searchwindowsserver/definition/Windows-NT (Accessed: 15 February 2024).

Bace, R. G. (2012) "Intrusion Detection and Intrusion Prevention Devices" In: Bosworth, S., Kabay, M. and Whyne, E., eds., 2012. *Computer Security Handbook*. Wiley & Sons, Hoboken, NJ, pp. 21.1-27.18.

Bales, R. (2023). "The First Computer Virus of Bob Thomas Explained: Everything You Need to Know", [online], History Computer, https://history-computer.com/the-first-computer-virus-of-bob-thomas/ (Accessed: 15 February 2024).

Bellovin, S. M., Cheswick, W., R. and Rubin, A. D. (1994) *Firewalls and Internet Security*, Addison-Wesley, Reading, MA.

Beyond Identity. (2021) "The history and future of passwords", [online], https://www.beyondidentity.com/blog/history-and-future-passwords (Accessed: 15 February 2024).

Biene-Hershey, M. v. (2007) "IT Security and IT Auditing between 1960 and 2000", in: De Leeuw, K. and Bergstra, J., eds. 2007. *The History of Information Security*. Elsevier, Amsterdam pp. 655-680.

Brenner, S. W. (2007) "History of Computer Crime", in: De Leeuw, K. and Bergstra, J., eds. 2007. *The History of Information Security*. Elsevier, Amsterdam pp. 705-721.

CCCS, Canadian Centre for Cyber Security (2020) *"Baseline cyber security controls for small and medium organizations*" [online], https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations (Accessed: 15 February 2024).

CISA, Cybersecurity and Infrastructure Security Agency (2023) "*Cybersecurity Advisory AA23-278A: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations*", [online], https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a (Accessed: 15 February 2024).

Cohen, F. (1987) Computer Viruses: Theory and Experiments, *Computers & Security*, Vol. 6, Issue 1, pp. 22-25.

Computer History Museum (no date), "*Timeline of Computer History*", [online], https://www.computerhistory.org/timeline/networking-the-web/ (Accessed: 15 February 2024).

de Fremery, R. (2021). "The evolution of multi-factor authentication", [online], LastPass, https://blog.lastpass.com/2021/12/the-evolution-of-multi-factor-authentication/ (Accessed: 15 February 2024).

DeNardis, L. (2007) "A History of Internet Security", in: De Leeuw, K. and Bergstra, J., eds. 2007. *The History of Information Security*. Elsevier, Amsterdam pp. 681-704.

Drake, B. (2020) "Exploring the Origins and Evolution of Vulnerability Management", [online], https://blog.igicybersecurity.com/origins-and-evolution-of-vulnerability-management (Accessed 19 February 2024).

Ferguson, P., Senie, D. (2000) Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, Request for Comments: 2827, [online], Network Working Group, https://datatracker.ietf.org/doc/html/rfc2827 (Accessed 19 February 2024).

Freiberger, P. A. and Swaine, M. R. (no date) "History of Computing", [online], Encyclopaedia Britannica, https://www.britannica.com/technology/computer/Time-sharing-and-minicomputers (Accessed: 15 February 2024).

IEEE Standards Association (2023) "IEEE 802.1X-2023: Port-based network access control" [Standard] https://www.ieee802.org/1/pages/802.1x-rev.html (Accessed: 15 February 2024).

Hayden, E. (2009) "Philosophy of Information Security: a Security Professional's Perspective", [online], Risk and Resilience Hub, https://www.riskandresiliencehub.com/philosophy-of-information-security-a-security-professionals-perspective/ (Accessed 19 February 2024).

Kindervag, J. (2016) "No More Chewy Centers: The Zero Trust Model of Information Security", [online], Forrester, https://www.forrester.com/report/No-More-Chewy-Centers-The-Zero-Trust-Model-Of-Information-Security/RES56682 (Accessed; 19 February 2024).

Lewis, R. (2024) "Cisco Systems" [online], Encyclopaedia Britannica, https://www.britannica.com/topic/Cisco-Systems-Inc (Accessed: 15 February 2024).

Linden, T. (1976) "Operating system structures to support security and reliable software" [online], National Institute of Standards and Technology, https://www.nist.gov/publications/operating-system-structures-support-security-and-reliable-software (Accessed 19. February 2024).

Meijer, H., Hoepman, J. H., Jacobs, B., & Poll, E. (2007) "Computer Security through Correctness and Transparency" In: De Leeuw, K. and Bergstra, J., eds. 2007. *The History of Information Security*. Elsevier, Amsterdam pp. 637-653.

MIT (n.d.) "Multics - Multiplexed Information and Computing Service", [online], MIT, https://web.mit.edu/multics-history/ (Accessed: 15 February 2024).

Zioni, M. (2022) "3 Must Haves When Implementing DevSecOps", [online], DevOps, https://devops.com/3-must-haves-when-implementing-devsecops/ (Accessed: 19 February 2024).

Mujović, V. (2018) "The History of VPN", [online], Le VPN, https://www.le-vpn.com/history-of-vpn/ (Accessed: 15 February 2024).

National Science Foundation (1991) "Computers at Risk: Safe Computing in the Information Age" [online], https://nap.nationalacademies.org/read/1581/chapter/1#iii (Accessed: 19. February 2022).

NIST, National Institute of Standards and Technology. (2020) "Control Baselines for Information Systems and Organizations", [online], Department of Commerce, NIST Special Publication 800-53B. https://doi.org/10.6028/NIST.SP.800-53B (Accessed 19 February 2024).

Neumann, P. G. et al. (1975) *A Provably Secure Operating System*, United States of America, Department of Defense.

Perry, Dennis G., Blumenthal, Steven H. and Hinden, Robert M. (1988) "The ARPANET and the DARPA Internet", *Library Hi Tech*, Vol 6, No 2, pp. 51-62.

Piscitello, D. M. and Chapin, A. L. (1993) *Open Systems Networking TCP/IP and OSI*, Addison-Wesley, Reading, MA.

Sanger, D. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age, Crown.

Schneier, B. (2018) *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, Norton,

Schulze, M. (2018) *From Cyber-Utopia to Cyber-War: Normative Change in Cyberspace* [online], Friedrich Schiller University of Jena. https://www.db-thueringen.de/receive/dbt_mods_00035107.

Vance, J. (2022) "What is a VLAN and how does it work?", [online], NETWORKWORLD, https://www.networkworld.com/article/971100/what-is-a-vlan-and-how-does-it-work.html (Accessed: 15 February 2024).

von Solms, R. (1998) "Information security management (3): the Code of Practice for Information Security Management (BS 7799)", *Information Management & Computer Security*, Vol. 6 No. 5, pp. 224-225.

Viegas, V., Kuyucu, O. (2022) *IT Security Controls. A Guide to Corporate Standards and Frameworks*, Apress Berkely, CA.

Vyssotsky, V., (1961) *Darwin: A Game of Survival and (Hopefully) Evolution*, Bell Telephone Laboratories, New Jersey.

Ware, W. (1970) *Security Controls for Computer Systems,* United States of America, Department of Defense.

Yost, J. R. (2007) "History of Computer Security Standards", in: De Leeuw, K. and Bergstra, J., eds. 2007. *The History of Information Security*. Elsevier, Amsterdam pp. 595-621.